# Executive Master's Degree

## Corporate Cybersecurity Policy Management

MCCPM

tech technological university

tech technological university

# Executive Master's Degree
## Corporate Cybersecurity Policy Management

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**
- Target Group: **Graduates who have previously completed any of the degrees in the fields of Social and Legal Sciences, Administration and Business.**

Website: **www.techtitute.com/pk/school-of-business/master/corporate-cybersecurity-policy-management**

# Index

01

# Welcome

Today, losses due to cyber-attacks are estimated to be well into the millions. Such is the exposure to cyber-attack that even states can be targeted by cyberincidents. This has highlighted the importance of having managers who are specialized in Cybersecurity Policy Management, with the right knowledge in organization, implementation and monitoring tools to coordinate all cybersecurity efforts. This program prepares the manager to face uncertain scenarios with confidence and advanced knowledge, providing quality solutions in IT Security. Through exhaustive theoretical content, based on real practical cases, you will obtain a modern and comprehensive perspective of all the functions that a cybersecurity manager must perform. All of this in a 100% online format, free of face-to-face classes and fixed schedules, with total flexibility.

**Master's Degree in Corporate Cybersecurity Policy Management.**
**TECH Technological University**

*It brings incalculable value to your Cybersecurity Policies by providing you with advanced knowledge of all the nuances, from the security systems themselves to the procedures in threat analysis that will give you the keys to position yourself with an advantage in your organization"*

02

# Why Study at TECH?

TECH is the world's largest 100% online business school. It is an elite business school, with a model based on the highest academic standards. A world-class centre for intensive managerial skills training.

*TECH is a university at the forefront of technology, and puts all its resources at the student's disposal to help them achieve entrepreneurial success"*

## At TECH Technological University

### Innovation

The university offers an online learning model that combines the latest educational technology with the most rigorous teaching methods. A unique method with the highest international recognition that will provide students with the keys to develop in a rapidly-evolving world, where innovation must be every entrepreneur's focus.

"Microsoft Europe Success Story", for integrating the innovative, interactive multi-video system.

### The Highest Standards

Admissions criteria at TECH are not economic. Students don't need to make a large investment to study at this university. However, in order to obtain a qualification from TECH, the student's intelligence and ability will be tested to their limits. The institution's academic standards are exceptionally high...

**95%** | **of TECH students successfully complete their studies**

### Networking

Professionals from countries all over the world attend TECH, allowing students to establish a large network of contacts that may prove useful to them in the future.

**100,000+**
**executives trained each year**

**200+**
**different nationalities**

### Empowerment

Students will grow hand in hand with the best companies and highly regarded and influential professionals. TECH has developed strategic partnerships and a valuable network of contacts with major economic players in 7 continents.

**500+** | **collaborative agreements with leading companies**

### Talent

This program is a unique initiative to allow students to showcase their talent in the business world. An opportunity that will allow them to voice their concerns and share their business vision.

After completing this program, TECH helps students show the world their talent.

### Multicultural Context

While studying at TECH, students will enjoy a unique experience. Study in a multicultural context. In a program with a global vision, through which students can learn about the operating methods in different parts of the world, and gather the latest information that best adapts to their business idea.

TECH students represent more than 200 different nationalities.



## Learn with the best

In the classroom, TECH's teaching staff discuss how they have achieved success in their companies, working in a real, lively, and dynamic context. Teachers who are fully committed to offering a quality specialization that will allow students to advance in their career and stand out in the business world.

Teachers representing 20 different nationalities.

*"At TECH, you will have access to the most rigorous and up-to-date case studies in the academic community"*

**TECH strives for excellence and, to this end, boasts a series of characteristics that make this university unique:**

## Analysis

TECH explores the student's critical side, their ability to question things, their problem-solving skills, as well as their interpersonal skills.

## Academic Excellence

TECH offers students the best online learning methodology. The university combines the Relearning method (a postgraduate learning methodology with the highest international rating) with the Case Study. A complex balance between tradition and state-of-the-art, within the context of the most demanding academic itinerary.

## Economy of Scale

TECH is the world's largest online university. It currently boasts a portfolio of more than 10,000 university postgraduate programs. And in today's new economy, **volume + technology = a ground-breaking price**. This way, TECH ensures that studying is not as expensive for students as it would be at another university.

03

# Why Our Program?

Studying this TECH program means increasing the chances of achieving professional success in senior business management.

It is a challenge that demands effort and dedication, but it opens the door to a promising future. Students will learn from the best teaching staff and with the most flexible and innovative educational methodology.

*We have highly qualified teachers and the most complete syllabus on the market, which allows us to offer you training of the highest academic level"*

**This program will provide students with a multitude of professional and personal advantages, particularly the following:**

01

## A significant career boost

By studying at TECH, students will be able to take control of their future and develop their full potential. By completing this program, students will acquire the skills required to make a positive change in their career in a short period of time.

*70% of participants achieve positive career development in less than 2 years.*

02

## Develop a strategic and global vision of companies

TECH offers an in-depth overview of general management to understand how each decision affects each of the company's different functional areas.

*Our global vision of companies will improve your strategic vision.*

03

## Consolidate the student's senior management skills

Studying at TECH means opening the doors to a wide range of professional opportunities for students to position themselves as senior executives, with a broad vision of the international environment.

*You will work on more than 100 real senior management cases.*

04

## Take on new responsibilities

The program will cover the latest trends, advances and strategies, so that students can carry out their professional work in a changing environment.

*45% of graduates are promoted internally.*

05

### Access to a powerful network of contacts

TECH connects its students to maximize opportunities. Students with the same concerns and desire to grow. Therefore, partnerships, customers or suppliers can be shared.

*You will find a network of contacts that will be instrumental for professional development.*

06

### Thoroughly develop business projects

Students will acquire a deep strategic vision that will help them develop their own project, taking into account the different areas in companies.

*20% of our students develop their own business idea.*

07

### Improve soft skills and management skills

TECH helps students apply and develop the knowledge they have acquired, while improving their interpersonal skills in order to become leaders who make a difference.

*Improve your communication and leadership skills and enhance your career.*

08

### Be part of an exclusive community

Students will be part of a community of elite executives, large companies, renowned institutions, and qualified professors from the most prestigious universities in the world: the TECH Technological University community.

*We give you the opportunity to train with a team of world renowned teachers.*

04

# Objectives

Cybersecurity being a crucial aspect in the development of any modern company, the objective of the present program could not be other than to offer the best possible program in Corporate Cybersecurity Policy Management. To this end, the group of computer experts has compiled exhaustive educational material that is fully focused on enhancing the skills, competencies and abilities of the manager.

*Lead your organization's cybersecurity by learning the ins and outs of the most effective cybersecurity policies"*

## TECH makes the goals of their students their own goals too. Working together to achieve them.

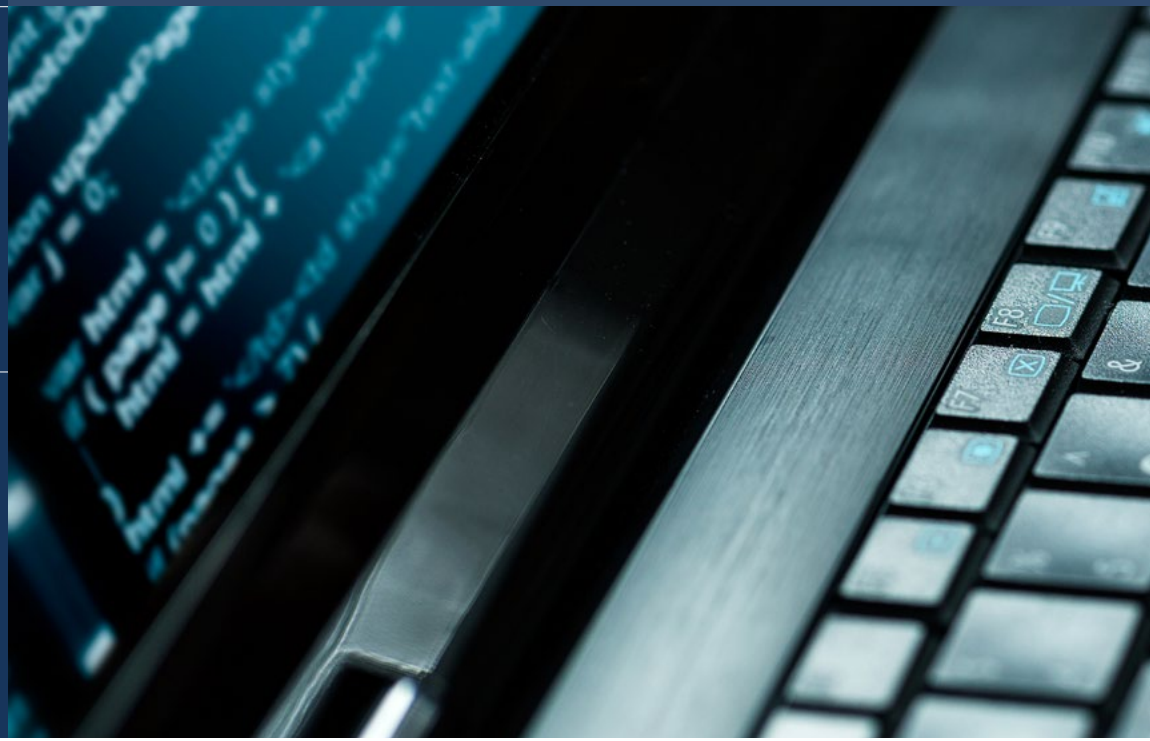
The **Master's Degree in Corporate Cybersecurity Policy Management** will program the student to:

01 Study the key concepts of information security in great detail

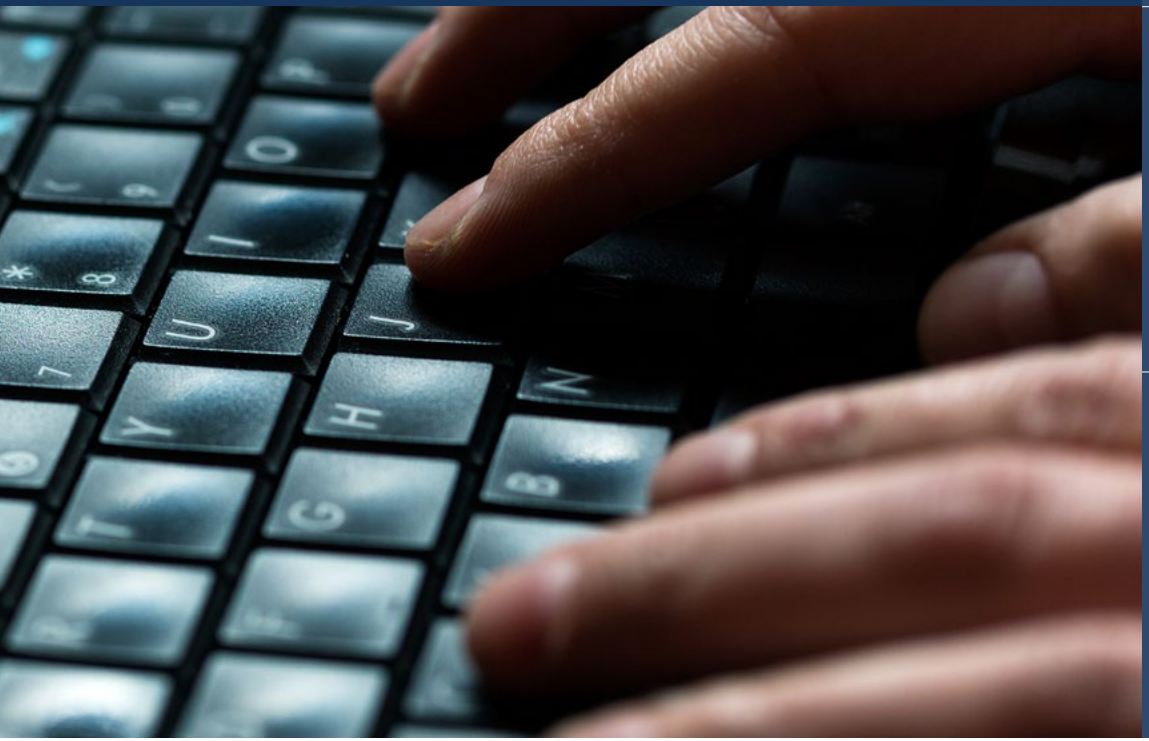
02 Analyze the regulations and standards currently applicable to ISMS

03 Implement an ISMS in the company

04 Determine which departments should be covered by the implementation of the safety management system



05 Develop the necessary measures to ensure good information security practices



06 Determine what authentication and i dentification are

07 Analyze the different authentication methods available and their practical implementation

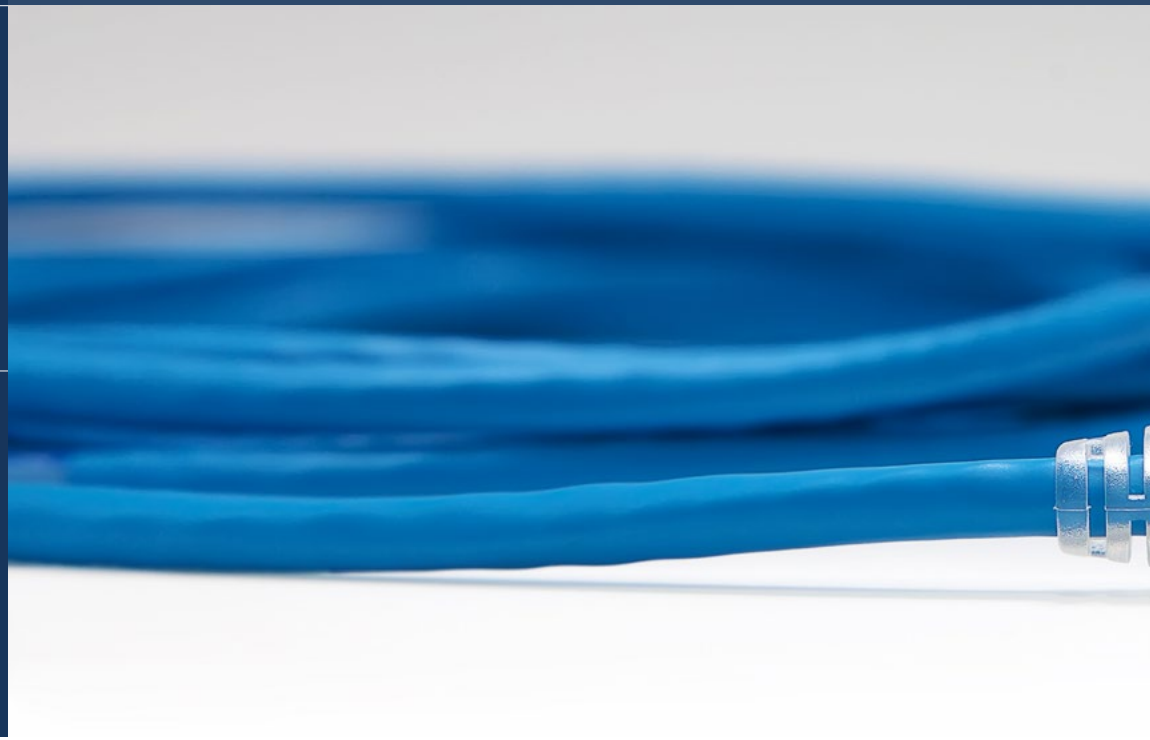
08 Implement the correct access control policy to software and systems

09 Develop specialized knowledge on how to manage incidents caused by IT security events

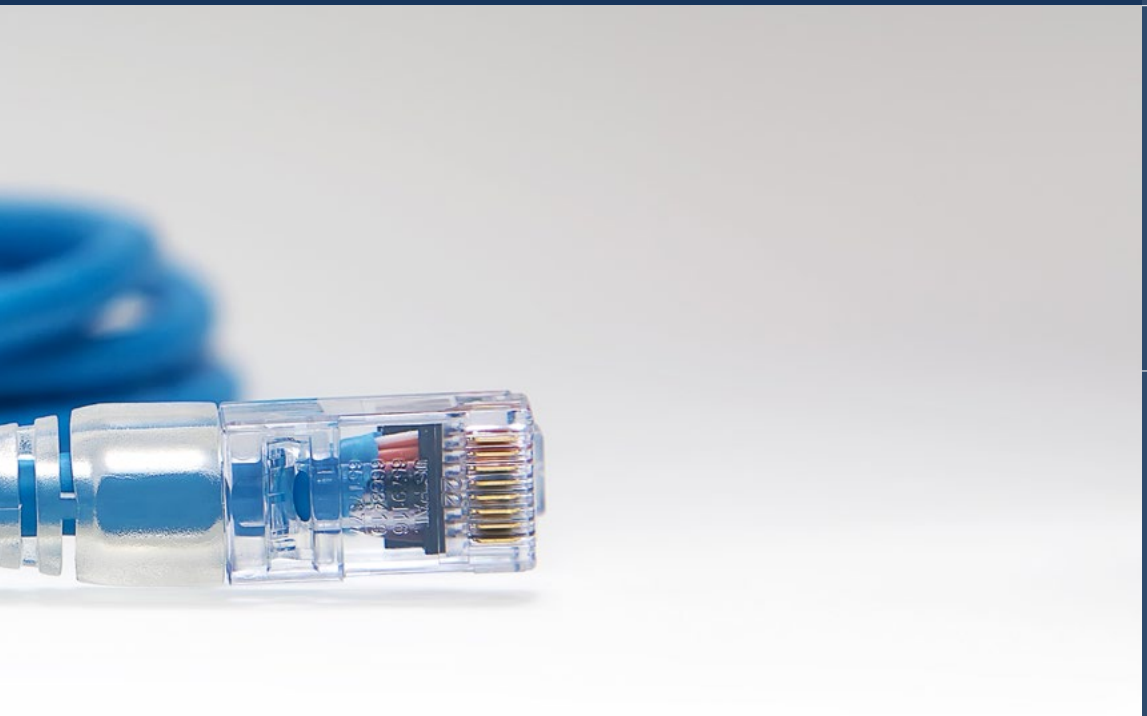
10 Analyze the terms 'safe area' and 'safe perimeter'

11 Analyze the different encryption algorithms used in communication networks

12 Determine the different real attacks to our information system



13 Evaluate the various security policies to mitigate attacks



14 Develop the concept of monitoring and implementation of metrics

15 Generate specialized knowledge on the concept of information security continuity

16 Determining what cryptography is and types of cryptography

05

# Skills

In order to carry out proper Cybersecurity Policy Management, it is essential to have great organizational abilities, in addition to possessing expert knowledge and skills in IT and technological matters. This is why, throughout this program, the manager will not only find a useful reference guide for IT security management, but they will also enhance their leadership and administrative management skills.

*You will hone the skills required to excel as an expert manager in Cybersecurity Policy, giving you a head start in senior management positions"*

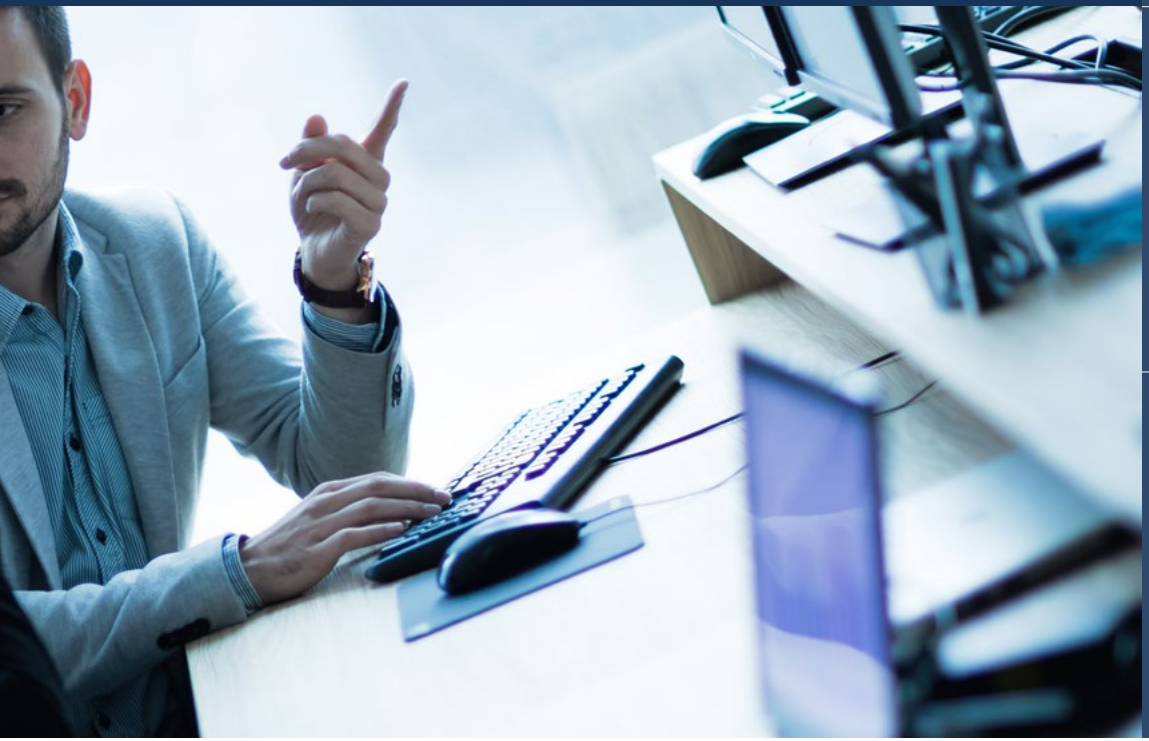
01 Determine the involvement of an ISMS in the internal organization of the entity, as well as its status

02 Establish security policies in the company

03 Determine what measures we need to implement with suppliers and maintenance of information systems

04 Generate specialized knowledge on threat control

05 Determine the phases of preventive threat management



06 Develop methodologies for computer threat analysis

07 Classify threats by impact and severity

08 Design a proprietary methodology for the analysis and preventive control of threats

09 Implement a correct policy with regards to access to networks and services

10 Analyze the importance of a correct treatment of security incidents

11 Compile the different biometric systems that exist

12 Examine Biometrics and Biometric Systems


13 Implement the correct physical security policies and physical access control systems in data centers

14 Implement a secure network

15 Examine the vulnerabilities of mobile and IoT platforms and how to avoid them

16 Establish the types of social engineering and learn how to mitigate them

17 Analyze the concept of monitoring and implementation of metrics

18 Determine the need for information security continuity

06

# Structure and Content

TECH has structured this program based on the Re-learning methodology, which means that the manager will not have to spend long hours of study to acquire all the proposed knowledge. Key terms and concepts in Cybersecurity Policies are given in a natural and reiterative way throughout the program, which ends up resulting in a much more progressive learning.

*You will be free to enter the virtual classroom 24 hours a day, being able to choose and adapt the pace of your studies to your own interests"*

## Syllabus

The Master's Degree in Corporate Cybersecurity Policy Management of TECH Technological University is an intensive program that prepares students for the most demanding areas of business cybersecurity.

The content of the Executive Master's Degree in Corporate Cybersecurity Policy Management is designed to promote the development of managerial skills that enable more rigorous decision-making in uncertain environments.

This Professional Master's Degree deals in depth with the digital world, security in this environment and the implementation of e-commerce in companies, and is designed to train professionals who understand Corporate Cybersecurity Policy Management, from a strategic, international and innovative perspective.

This Executive Master's Degree takes place over 12 months and is divided into 10 modules:

| | |
|---|---|
| **Module 1** | Information Security Management System (ISMS) |
| **Module 2** | Organizational Aspects of Information Security Policy |
| **Module 3** | Security Policies for the Analysis of Threats in Computer Systems |
| **Module 4** | Practical Implementation of Software and Hardware Security Policies |
| **Module 5** | Security Incident Management Policies |
| **Module 6** | Implementation of Physical and Environmental Safety Policies in the Company |
| **Module 7** | Secure Communications Policies in the Company |
| **Module 8** | Practical Implementation of Security Policies against Attacks |
| **Module 9** | Information Systems Security Policy Monitoring Tools |
| **Module 10** | Practical Security Disaster Recovery Policy |

## Where, When and How is it Taught?

TECH offers the possibility of developing this Executive Master's Degree in Corporate Cybersecurity Policy Management completely online. Over the course of 12 months, you will be able to access all the contents of this program at any time, allowing you to self-manage your study time.

*A unique, key, and decisive educational experience to boost your professional development and make the definitive leap.*

## **Module 1.** Information Security Management System

### 1.1. Information Security Key Aspects
1.1.1. Information Security
1.1.1.1. Confidentiality
1.1.1.2. Integrity
1.1.1.3. Availability
1.1.1.4. Information Security Measurements

### 1.2. Information Security Management Systems
1.2.1. Information Security Management Models
1.2.2. Documents to Implement an ISMS
1.2.3. Levels and Controls of an ISMS

### 1.3. International Norms and Standards
1.3.1. International Standards in Information Security
1.3.2. Origin and Evolution of the Standard
1.3.3. International Information Security Management Standards
1.3.4. Other Reference Standards

### 1.4. ISO/IEC 27,000 Standards
1.4.1. Purpose and Areas of Application
1.4.2. Structure of the Standard
1.4.3. Certification
1.4.4. Accreditation Phases
1.4.5. Benefits of ISO/IEC 27,000 Standards

### 1.5. Design and Implementation of a General Information Security System
1.5.1. Design and Implementation of a General Information Security System
1.5.2. Phases of Implementation of a General Information Security System
1.5.3. Business Continuity Plans

### 1.6. Phase I: Diagnosis
1.6.1. Preliminary Diagnosis
1.6.2. Identification of the Stratification Level
1.6.3. Level of Compliance with Standards/Norms

### 1.7. Phase II: Preparation
1.7.1. Context of the Organization
1.7.2. Analysis of Applicable Safety Regulations
1.7.3. Scope of the General Information Security System
1.7.4. General Information Security System Policy
1.7.5. Objectives of the General Information Security System

### 1.8. Phase III: Planning
1.8.1. Asset Classification
1.8.2. Risk Assessment
1.8.3. Identification of Threats and Risks

### 1.9. Phase IV: Implementation and Follow-up
1.9.1. Analysis of Results
1.9.2. Assigning Responsibilities
1.9.3. Timing of the Action Plan
1.9.4. Monitoring and Audits

### 1.10. Incident Management Security Policies
1.10.1. Phases
1.10.2. Incident Categorization
1.10.3. Incident Management and Procedures

**Module 2.** Organizational Aspects of Information Security Policy

### 2.1. Internal Organization
2.1.1. Assigning Responsibilities
2.1.2. Segregation of Duties
2.1.3. Contacts with Authorities
2.1.4. Information Security in Project Management

### 2.2. Asset Management
2.2.1. Liability for Assets
2.2.2. Classification of Information
2.2.3. Handling of Storage Media

### 2.3. Security Policies in Business Processes
2.3.1. Analysis of the Vulnerabilities of Business Processes
2.3.2. Business Impact Analysis
2.3.3. Classification of Processes with Respect to Business Impact

### 2.4. Security Policies Linked to Human Resources
2.4.1. Before Hiring
2.4.2. During Contracting
2.4.3. Termination or Change of Position

### 2.5. Management Security Policies
2.5.1. Management Guidelines on Information Security
2.5.2. BIA - Analyzing the Impact
2.5.3. Recovery Plan as a Security Policy

### 2.6. Acquisition and Maintenance of Information Systems
2.6.1. Information Systems Security Requirements
2.6.2. Development and Support Data Security
2.6.3. Test Data

### 2.7. Security with Suppliers
2.7.1. IT Security with Suppliers
2.7.2. Management of Service Delivery with Assurance
2.7.3. Supply Chain Security

### 2.8. Operational Safety
2.8.1. Operational Responsibilities
2.8.2. Protection Against Malicious Code
2.8.3. Backup Copies
2.8.4. Activity and Supervision Records

### 2.9. Safety and Regulatory Management
2.9.1. Safety and Regulatory Management
2.9.2. Compliance with Legal Requirements
2.9.3. Information Security Reviews

### 2.10. Business Continuity Management Security
2.10.1. Business Continuity Management Security
2.10.2. Continuity of Information Security
2.10.3. Redundancies

**Module 3.** Security Policies for the Analysis of Threats in Computer Systems

### 3.1. Threat Management in Security Policies
3.1.1. Risk Management
3.1.2. Security Risk
3.1.3. Threat Management Methodologies
3.1.4. Implementation of Methodologies

### 3.2. Phases of Threat Management
3.2.1. Identification
3.2.2. Analysis
3.2.3. Localisation
3.2.4. Safeguard Measures

### 3.3. Audit Systems for Threat Localization
3.3.1. Threat Location Auditing Systems
3.3.2. Classification and Information Flow
3.3.3. Analysis of Vulnerable Processes

### 3.4. Risk Classification
3.4.1. Types of Risk
3.4.2. Calculation of Threat Probability
3.4.3. Residual Risk

### 3.5. Risk Treatment
3.5.1. Risk Treatment
3.5.2. Implementation of Safeguard Measures
3.5.3. Transfer or Assume

### 3.6. Control Risks
3.6.1. Continuous Risk Management Process
3.6.2. Implementation of Security Metrics
3.6.3. Strategic Model of Information Security Metrics

### 3.7. Practical Methodologies for Threat Analysis and Control
3.7.1. Threat Catalog
3.7.2. Catalog of Control Measures
3.7.3. Safeguards Catalog

### 3.8. ISO 27005
3.8.1. Risk Identification
3.8.2. Risk Analysis
3.8.3. Risk Evaluation

### 3.9. Risk, Impact and Threat Matrix
3.9.1. Data, Systems and Personnel
3.9.2. Threat Probability
3.9.3. Magnitude of Damage

### 3.10. Design of Phases and Processes in Threat Analysis
3.10.1. Identification of Critical Organizational Elements
3.10.2. Determination of Threats and Impacts
3.10.3. Impact and Risk Analysis
3.10.4. Methods

**Module 4.** Practical Implementation of Software and Hardware Security Policies

### 4.1. Practical Implementation of Software and Hardware Security Policies
4.1.1. Implementation of Identification and Authorization
4.1.2. Implementation of Identification Techniques
4.1.3. Technical Authorization Measures

### 4.2. Identification and Authorization Technologies
4.2.1. Identifier and OTP
4.2.2. USB Token or PKI Smart Card
4.2.3. The "Confidential Defense" Key
4.2.4. Active RFID

### 4.3. Software and Systems Access Security Policies
4.3.1. Implementation of Access Control Policies
4.3.2. Implementation of Communications Access Policies
4.3.3. Types of Security Tools for Access Control

### 4.4. User Access Management
4.4.1. Access Rights Management
4.4.2. Segregation of Roles and Access Functions
4.4.3. Implementation of Access Rights in Systems

### 4.5. Access Control to Systems and Applications
4.5.1. Minimum Access Rule
4.5.2. Secure Logon Technologies
4.5.3. Password Security Policies

### 4.6. Identification Systems Technologies
4.6.1. Active Directory
4.6.2. OTP
4.6.3. PAP, CHAP
4.6.4. KERBEROS, DIAMETER, NTLM

### 4.7. CIS Controls for Systems Hardening
4.7.1. Basic CIS Controls
4.7.2. Fundamental CIS Controls
4.7.3. Organizational CIS Controls

### 4.8. Operational Safety
4.8.1. Protection Against Malicious Code
4.8.2. Backup Copies
4.8.3. Activity Log and Supervision

### 4.9. Management of Technical Vulnerabilities
4.9.1. Technical Vulnerabilities
4.9.2. Technical Vulnerability Management
4.9.3. Restrictions on Software Installation

### 4.10. Implementation of Security Policy Practices
4.10.1. Implementation of Security Policy Practices
4.10.2. Logical Vulnerabilities
4.10.3. Implementation of Defense Policies

**Module 5.** Security Incident Management Policies

5.1. Information Security Incident Management Policies and Enhancements
- 5.1.1. Incident Management
- 5.1.2. Responsibilities and Procedures
- 5.1.3. Event Notification

5.2. Intrusion Detection and Prevention Systems (IDS/IPS)
- 5.2.1. System Operating Data
- 5.2.2. Types of Intrusion Detection Systems
- 5.2.3. Criteria for IDS/IPS Placement

5.3. Security Incident Response
- 5.3.1. Data Collection Procedure
- 5.3.2. Intrusion Verification Process
- 5.3.3. CERT Organizations

5.4. Intrusion Attempt Notification and Management Process
- 5.4.1. Responsibilities in the Notification Process
- 5.4.2. Classification of Incidents
- 5.4.3. Resolution and Recovery Process

5.5. Forensic Analysis as a Security Policy
- 5.5.1. Volatile and Non-Volatile Evidence
- 5.5.2. Analysis and Collection of Electronic Evidence
  - 5.5.2.1. Analysis of Electronic Evidence
  - 5.5.2.2. Collection of Electronic Evidence

5.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
- 5.6.1. Snort
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. Event Centralizing Tools
- 5.7.1. SIM
- 5.7.2. SEM
- 5.7.3. SIEM

5.8. CCN-STIC Security Guide 817
- 5.8.1. CCN-STIC Security Guide 817
- 5.8.2. Cyber Incident Management
- 5.8.3. Metrics and Indicators

5.9. NIST SP800-61
- 5.9.1. Computer Security Incident Response Capability
- 5.9.2. Handling an Incident
- 5.9.3. Coordination and Information Sharing

5.10. ISO 27035
- 5.10.1. ISO 27035 Standard. Incident Management Principles
- 5.10.2. Incident Management Plan Preparation Guidelines
- 5.10.3. Incident Response Operations Guides

**Module 6.** Implementation of Physical and Environmental Safety Policies in the Company

6.1. Security Areas
6.1.1. Physical Security Perimeter
6.1.2. Working in Safe Areas
6.1.3. Security of Offices, Offices and Resources

6.2. Physical Input Controls
6.2.1. Physical Input Controls
6.2.2. Physical Access Control Policies
6.2.3. Physical Input Control Systems

6.3. Physical Access Vulnerabilities
6.3.1. Physical Access Vulnerabilities
6.3.2. Main Physical Vulnerabilities
6.3.3. Implementation of Safeguards Measures

6.4. Physiological Biometric Systems
6.4.1. Fingerprint
6.4.2. Facial Recognition
6.4.3. Iris and Retinal Recognition
6.4.4. Other Physiological Biometric Systems

6.5. Biometric Behavioral Systems
6.5.1. Signature Recognition
6.5.2. Writer Recognition
6.5.3. Voice Recognition
6.5.4. Other Biometric Behavioral Systems

6.6. Biometrics Risk Management
6.6.1. Biometrics Risk Management
6.6.2. Implementation of Biometric Systems
6.6.3. Vulnerabilities of Biometric Systems

6.7. Implementation of Policies in Hosts
6.7.1. Installation of Supply and Security Cabling
6.7.2. Equipment Location
6.7.3. Exit of the Equipment Outside the Premises
6.7.4. Unattended Computer Equipment and Clear Post Policy

6.8. Environmental Protection
6.8.1. Fire Protection Systems
6.8.2. Earthquake Protection Systems
6.8.3. Earthquake Protection Systems

6.9. Data Processing Center Security
6.9.1. Security Doors
6.9.2. Video Surveillance Systems (CCTV)
6.9.3. Safety Control

6.10. International Physical Security Regulations
6.10.1. IEC 62443-2-1 (European)
6.10.2. NERC CIP-005-5 (USA)
6.10.3. NERC CIP-014-2 (USA)

## **Module 7.** Secure Communications Policies in the Company

### 7.1. Network Security Management
7.1.1. Network Control and Monitoring
7.1.2. Segregation of Networks
7.1.3. Network Security Systems

### 7.2. Secure Communication Protocols
7.2.1. TCP/IP Model
7.2.2. IPSEC Protocol
7.2.3. TLS Protocol

### 7.3. Protocol TLS 1.3
7.3.1. Phases of a TLS1.3 Process
7.3.2. Handshake Protocol
7.3.3. Registration Protocol
7.3.4. Differences with TLS 1.2

### 7.4. Cryptographic Algorithms
7.4.1. Cryptographic Algorithms Used in Communications
7.4.2. Cipher-Suites
7.4.3. Cryptographic Algorithms allowed for TLS 1.3

### 7.5. Digest Functions
7.5.1. Digest Functions
7.5.2. MD6
7.5.3. SHA

### 7.6. PKI. Public Key Infrastructure
7.6.1. PKI and its Entities
7.6.2. Digital Certificate
7.6.3. Types of Digital Certificates

### 7.7. Tunnel and Transport Communications
7.7.1. Tunnel Communications
7.7.2. Transport Communications
7.7.3. Encrypted Tunnel Implementation

### 7.8. SSH. Secure Shell
7.8.1. SSH. Safe Capsule
7.8.2. SSH Functions
7.8.3. SSH Tools

### 7.9. Audit of Cryptographic Systems
7.9.1. Audit of Cryptographic Systems
7.9.2. Integration Test
7.9.3. Cryptographic System Testing

### 7.10. Cryptographic Systems
7.10.1. Cryptographic Systems
7.10.2. Cryptographic Systems Vulnerabilities
7.10.3. Cryptographic Safeguards

## **Module 8.** Practical Implementation of Security Policies against Attacks

### 8.1. System Hacking
8.1.1. System Hacking
8.1.2. Risks and Vulnerabilities
8.1.3. Countermeasures

### 8.2. DoS Attack
8.2.1. DoS Attack
8.2.2. Risks and Vulnerabilities
8.2.3. Countermeasures

### 8.3. Session Hijacking
8.3.1. Session Hijacking
8.3.2. The Process of Hijacking
8.3.3. Hijacking Countermeasures

### 8.4. Evasion of IDS, Firewalls and Honeypots
8.4.1. Evaidng IDS, Firewalls and Honeypots
8.4.2. Avoidance Techniques
8.4.3. Implementation of Countermeasures

### 8.5. Hacking Web Servers
8.5.1. Hacking Web Servers
8.5.2. Attacks on Web Servers
8.5.3. Implementation of Defence Measures

### 8.6. Hacking Web Applications
8.6.1. Hacking Web Applications
8.6.2. Attacks on Web Applications
8.6.3. Implementation of Defence Measures

### 8.7. Hacking Wireless Networks
8.7.1. Hacking Wireless Networks
8.7.2. Vulnerabilities in Wi-Fi Networks
8.7.3. Implementation of Defense Measures

### 8.8. Hacking Mobile Platforms
8.8.1. Hacking Mobile Platforms
8.8.2. Vulnerabilities of Mobile Platforms
8.8.3. Implementation of Countermeasures

### 8.9. Ransomware
8.9.1. Ransomware
8.9.2. Vulnerabilities Causing Ransomware
8.9.3. Implementation of Countermeasures

### 8.10. Social Engineering
8.10.1. Social Engineering
8.10.2. Types of Social Engineering
8.10.3. Countermeasures for Social Engineering

## **Module 9.** Information Systems Security Policy Monitoring Tools

### 9.1. Information Systems Monitoring Policies
9.1.1. System Monitoring
9.1.2. Metrics
9.1.3. Types of Metrics

### 9.2. Systems Auditing and Registration
9.2.1. Systems Auditing and Registration
9.2.2. Windows Auditing and Logging
9.2.3. Linux Auditing and Logging

### 9.3. SNMP Protocol. Simple Network Management Protocol
9.3.1. SNMP Protocol
9.3.2. SNMP Functions
9.3.3. SNMP Tools

### 9.4. Network Monitoring
9.4.1. Network Monitoring
9.4.2. Network Monitoring in Control Systems
9.4.3. Monitoring Tools for Control Systems

### 9.5. Nagios. Network Monitoring System
9.5.1. Nagios
9.5.2. Operation of Nagios
9.5.3. Nagios Installation

### 9.6. Zabbix. Network Monitoring System
9.6.1. Zabbix.
9.6.2. How Zabbix Works
9.6.3. Zabbix Installation

### 9.7. Cacti. Network Monitoring System
9.7.1. Cacti
9.7.2. How Cacti Works
9.7.3. Installation of Cacti

### 9.8. Pandora. Network Monitoring System
9.8.1. Pandora.
9.8.2. Operation of Pandora
9.8.3. Pandora Installation

### 9.9. SolarWinds. Network Monitoring System
9.9.1. SolarWinds.
9.9.2. Operation of SolarWinds
9.9.3. Installation of SolarWinds

### 9.10. Monitoring Regulations
9.10.1. Monitoring Regulations
9.10.2. CIS Controls Over Auditing and Record Keeping
9.10.3. NIST 800-123 (U.S.A.)

## **Module 10.** Practical Security Disaster Recovery Policy

### 10.1. DRP. Disaster Recovery Plan
10.1.1. Objective of a DRP
10.1.2. Benefits of a DRP
10.1.3. Consequences of a Missing and Not up-to-Date DRP

### 10.2. Guidance for Defining a DRP (Disaster Recovery Plan)
10.2.1. Scope and Objectives
10.2.2. Recuperation Strategy Design
10.2.3. Assignment of Roles and Responsibilities
10.2.4. Inventorying Hardware, Software and Services
10.2.5. Tolerance for Downtime and Data Loss
10.2.6. Establishment of the Specific Types of DRP Required
10.2.7. Implementation of a Training, Awareness and Communication Plan

### 10.3. Scope and Objectives of a DRP (Disaster Recovery Plan)
10.3.1. Response Guarantee
10.3.2. Technological Components
10.3.3. Scope of the Continuity Policy

### 10.4. Disaster Recovery Plan (DRP) Strategy Design
10.4.1. Disaster Recovery Strategy
10.4.2. Budget
10.4.3. Human and Physical Resources
10.4.4. Management Positions at Risk
10.4.5. Technology
10.4.6. Data

### 10.5. Continuity of Information Processes
10.5.1. Continuity Planning
10.5.2. Continuity Implementation
10.5.3. Verification of Continuity Assessment

### 10.6. Scope of a BCP (Business Continuity Plan)
10.6.1. Determination of the Most Critical Processes
10.6.2. Asset-Based Approach
10.6.3. Process Approach

### 10.7. Implementation of Guaranteed Business Processes
10.7.1. Priority Activities (PA)
10.7.2. Ideal Recovery Times (IRT)
10.7.3. Survival Strategies

### 10.8. Organizational Analysis
10.8.1. Acquisition of information
10.8.2. Business Impact Analysis (BIA)
10.8.3. Risk Analysis in the Organization

### 10.9. Response to Contingency
10.9.1. Crisis Plan
10.9.2. Operational Environment Recovery Plans
10.9.3. Technical Work or Incident Procedures

### 10.10. International Standard ISO 27031 BCP
10.10.1. Objectives
10.10.2. Terms and Definitions
10.10.3. Operation

07

# Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**

This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

*Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"*

## TECH Business School uses the Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

*At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"*


*This program prepares you to face business challenges in uncertain environments and achieve business success.*

*Our program prepares you to face new challenges in uncertain environments and achieve success in your career.*

## A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch to present executives with challenges and business decisions at the highest level, whether at the national or international level. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and business reality is taken into account.

> *You will learn, through collaborative activities and real cases, how to solve complex situations in real business environments"*

The case method has been the most widely used learning system among the world's leading business schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question we face in the case method, an action-oriented learning method. Throughout the program, the studies will be presented with multiple real cases. They must integrate all their knowledge, research, argue and defend their ideas and decisions.

## Relearning Methodology

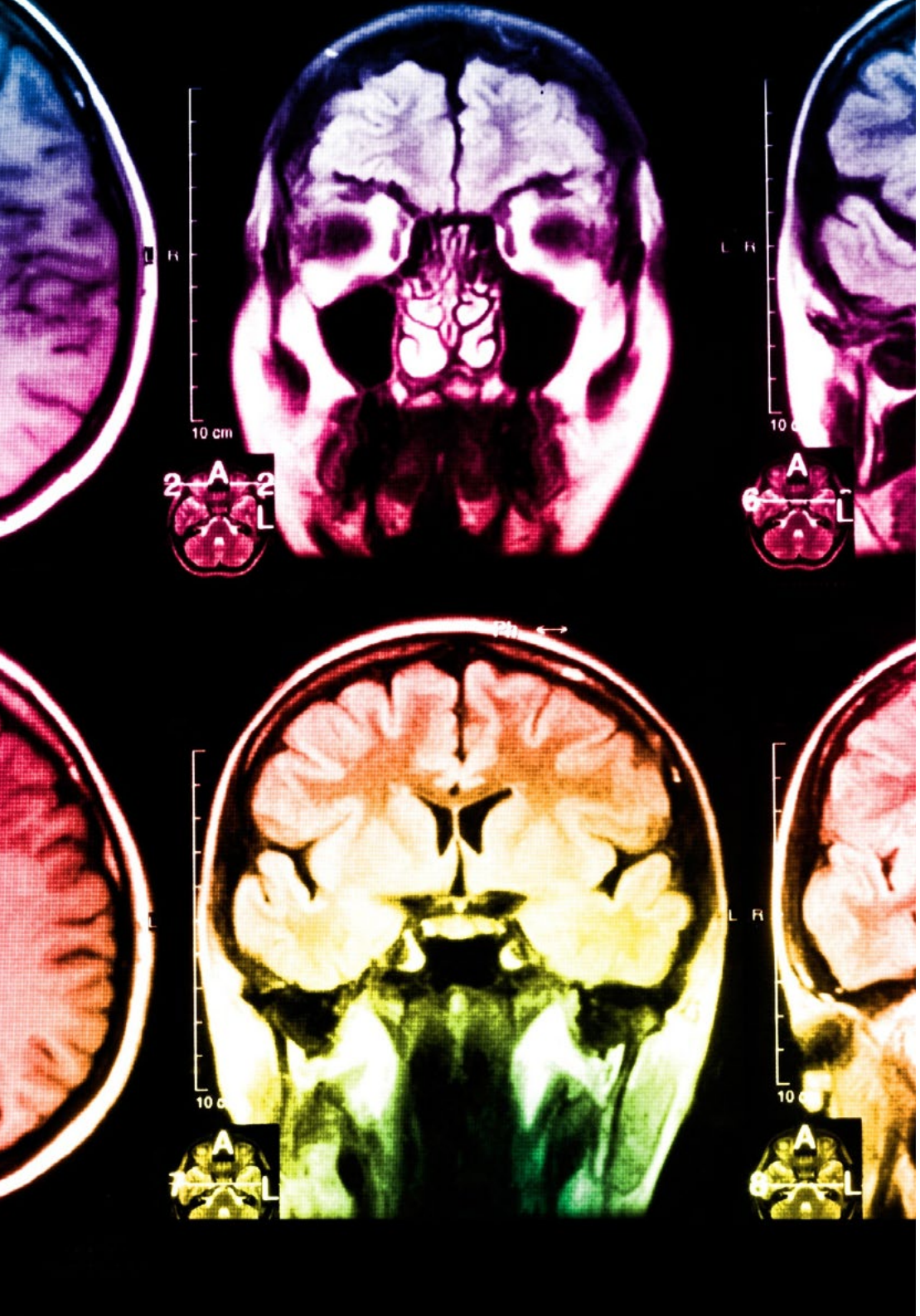
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

We enhance the Case Study with the best 100% online teaching method: Relearning.

*Our online system will allow you to organize your time and learning pace, adapting it to your schedule. You will be able to access the contents from any device with an internet connection.*

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our online business school is the only one in the world licensed to incorporate this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. With this methodology we have trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, markets, and financial instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

*Relearning will allow you to learn with less effort and better performance, involving you more in your specialization, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation to success.*

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

**This program offers the best educational material, prepared with professionals in mind:**

### Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

### Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

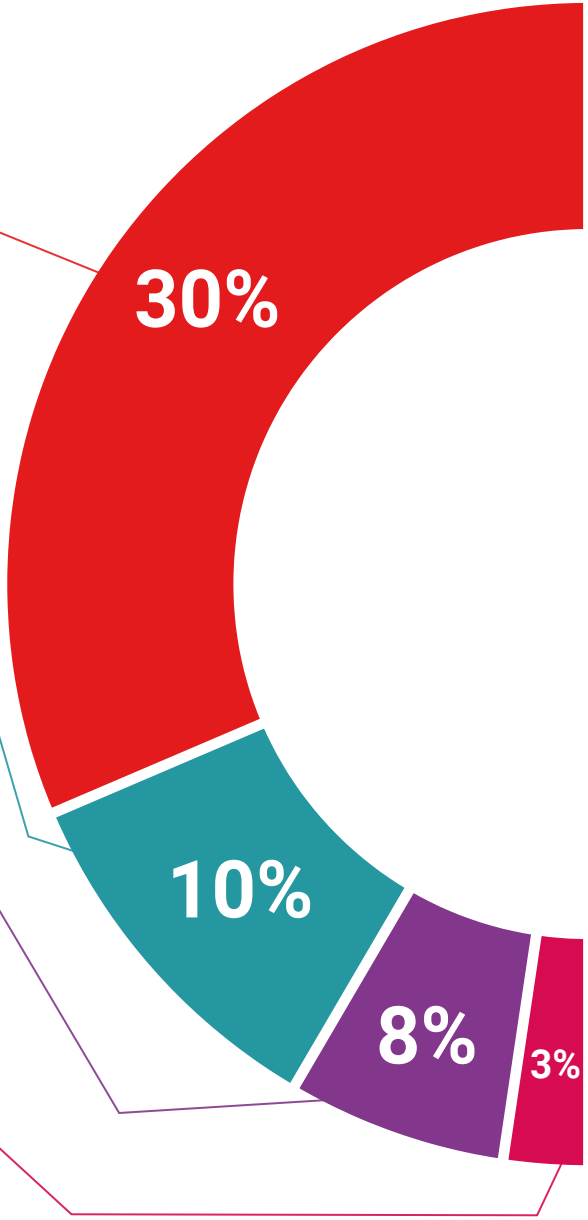
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

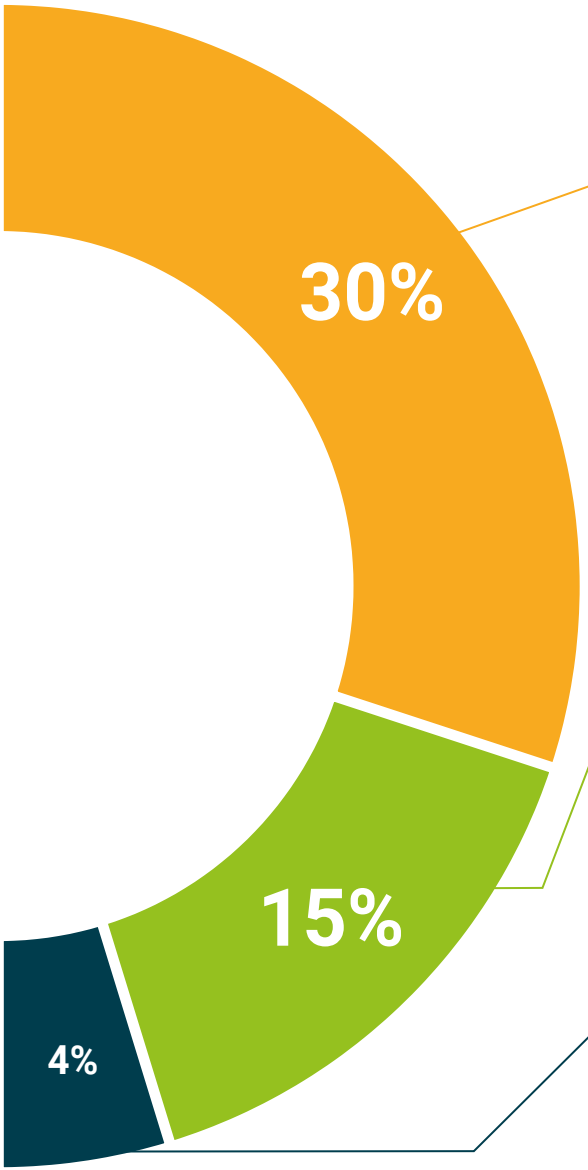
### Management Skills Exercises

They will carry out activities to develop specific executive competencies in each thematic area. Practices and dynamics to acquire and develop the skills and abilities that a high-level manager needs to develop in the context of the globalization we live in.

### Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.






### Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best senior management specialists in the world.

### Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

### Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

08

# Our Students' Profiles

The Executive Master's Degree is aimed at Graduates who have previously completed any of the following degrees in the field of Social and Legal Sciences, Administration and Economics.

This program uses a multidisciplinary approach as the students have a diverse set of academic profiles and represent multiple nationalities.

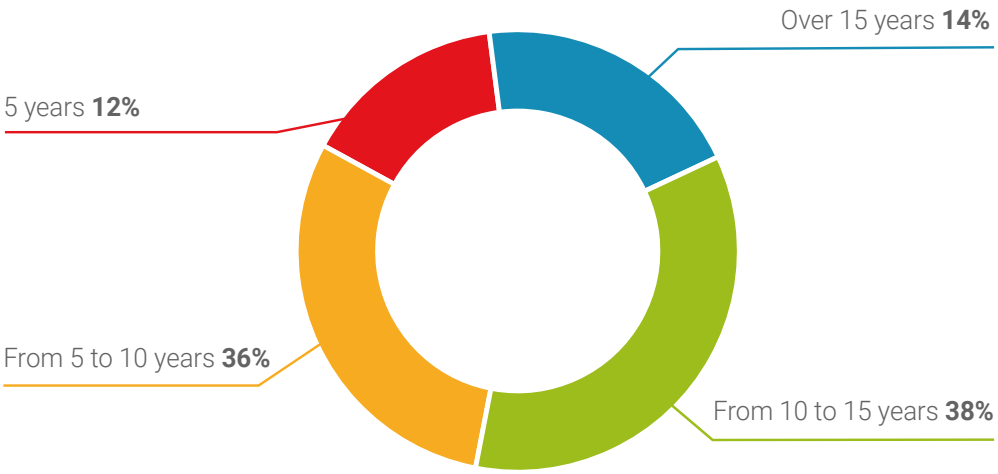
The Executive Master's Degree may also be taken by professionals who, being university graduates in any area, have two years of work experience in the field of Cybersecurity Policy Management.

*If you are looking to boost your professional career with quality knowledge, based on the most current reality of cybersecurity, enroll now in this program"*

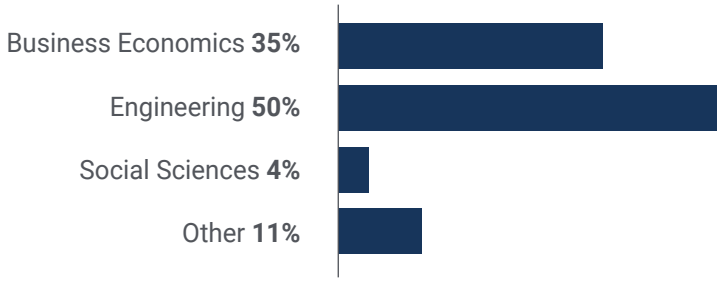
## Average Age

Between **35** and **45** years old

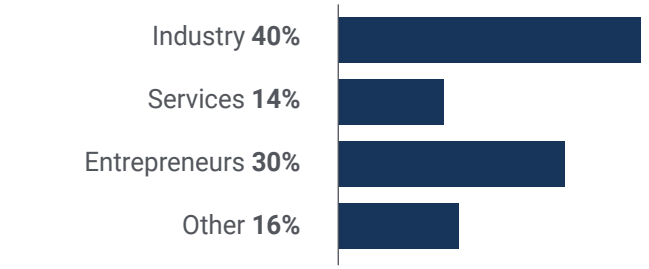
## Years of Experience



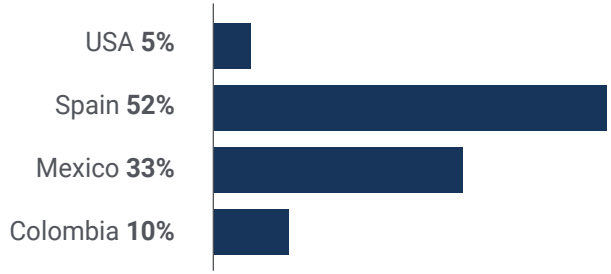

## Training




## Academic Profile



## Geographical Distribution




# Gabriel Gutiérrez Gómez

**Cybersecurity Manager**

*"After suffering a severe computer attack on our organization, we put more emphasis on protecting our databases and dedicated a small department to it. Thanks to this program, I was able to lead that effort, designing and implementing the cybersecurity policies we continue to use today."*

09

# Course Management

In order to achieve the highest possible quality of all the educational content, TECH has selected a group of teachers who are experts in the different areas covered by cybersecurity. Therefore, the manager will have access to a syllabus written by professionals with extensive experience in Cybersecurity Policy Management, who have contributed to all the theory with their distinctive practical vision for each of the topics covered.

*Rely on a teaching staff with experience in senior management and complex IT security management, with topics dedicated to information systems maintenance, forensic analysis and Hijacking".*

## Management

### Ms. Fernández Sapena, Sonia

- Chief Security Officer of the Universitat de les Illes Balears
- Senior Security Architect in different universities
- Head of IT Security at Sufi and Campus Extens of the UIB
- Graduated in Computer Engineering at the University of Alcalá de Henares
- Master in DevOps: Docker and Kubernetes at Cyber Business Center

## Professors

### Mr. Oropesiano Carrizosa, Francisco

- Web Services Manager/Email/DNS/Content Managers
- Network and Server Systems Security Technician
- Web Site Design and Production
- Graduated in Computer Engineering at the University of Alcalá de Henares
- Master in DevOps: Docker and Kubernetes at Cyber Business Center
- Master's Degree in Networks and Telecommunications

### Mr. Peralta Alonso, Jon

- Lawyer / DPO at Altia Consultores S.A.
- Lawyer / Legal Advisor at Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Commercial Manager at Kutxabank
- Graduated in Law at the Public University of the Basque Country
- Master's Degree in Data Protection Officer at EIS Innovative School
- Master's Degree in Advocacy at the Public University of the Basque Country

### Mr. Ortega López, Florencio

- ICT and Security Consultant in private and public companies.
- Graduated in Industrial Engineering at the University of Alcalá de Henares
- University Master's Degree for teachers at Unir
- MBA in Business Administration and Management by IDE-CESEM
- Master's Degree in Information Technology Direction and Management by IDE-CESEM

10

# Impact on Your Career

TECH is aware of the effort that the manager must make to take on a degree of these characteristics, so it devotes special effort to ensure that all content and teaching materials provided meet the highest quality standards. Thus, the multimedia library serves as an exceptional reference in the area of cybersecurity, and can even be downloaded in its entirety to continue using it once the degree is completed.

*You will achieve the economic and professional projection you are looking for thanks to the constant support of a teaching and technical team committed to take you to the zenith of management in Cybersecurity Policies"*

## Are you ready to take the leap? Excellent professional development awaits you

The Executive Master's Degree in Corporate Cybersecurity Policy Management of TECH is an intensive program that prepares students to face challenges and business decisions in the field of cybersecurity. Its main objective is to promote your personal and professional growth and help you achieve success.

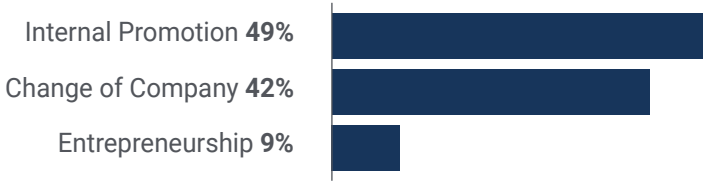
If you want to improve yourself, make a positive change at a professional level and interact with the best, this is the place for you.

*You will achieve the job improvement you are looking for in less time than you imagine thanks to TECH's pedagogical methodology.*

*Enroll now in this Executive Master's Degree and do not wait any longer to achieve a positive change in your environment.*

### When the change occurs


### Type of change



## Salary increase

The completion of this program represents a salary increase of more than **25%** for our students.

11

# Benefits for Your Company

The Executive Master's Degree in Corporate Cybersecurity Policy Management helps to elevate organizational talent to its full potential through the instruction of high-level leaders.

Participating in this Executive Master's Degree is a unique opportunity to access a powerful network of contacts in which to find future professional partners, customers or suppliers.

*Cyber threats are one of the greatest vulnerabilities to which companies of all types and sizes are exposed. Specialize in the area with the greatest future projection"*

**Developing and retaining talent in companies is the best long-term investment.**

01

### Intellectual Capital and Talent Growth

The professional will introduce the company to new concepts, strategies, and perspectives that can bring about significant changes in the organization.

02

### Retaining high-potential executives to avoid talent drain

This program strengthens the link between the company and the professional and opens new avenues for professional growth within the company.

03

### Building agents of change

You will be able to make decisions in times of uncertainty and crisis, helping the organization overcome obstacles.

04

### Increased international expansion possibilities

Thanks to this program, the company will come into contact with the main markets in the world economy.

05

### Project Development

The professional can work on a current project or develop new projects in the field of R&D or Business Development within their company.

06

### Increased competitiveness

This Professional Master's Degree will equip students with the skills to take on new challenges and drive the organization forward.

12

# Certificate

The Executive Master's Degree in Corporate Cybersecurity Policy Management guarantees, in addition to the most rigorous and up-to-date program, access to a Executive Master's Degree issued by TECH Technological University.

*Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"*

This **Executive Master's Degree in Corporate Cybersecurity Policy Management** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Executive Master's Degree** certificate issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the **Executive Master's Degree,** and meets the requirements commonly demanded by labor exchanges, competitive examinations, and professional career evaluation committees.

Title: **Executive Master's Degree in Corporate Cybersecurity Policy Management**

Official Nº of hours: **1,500 h.**


tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _____, with identification number _____.

For having successfully passed and accredited the following program

EXECUTIVE MASTER'S DEGREE

in

Corporate Cybersecurity Policy Management

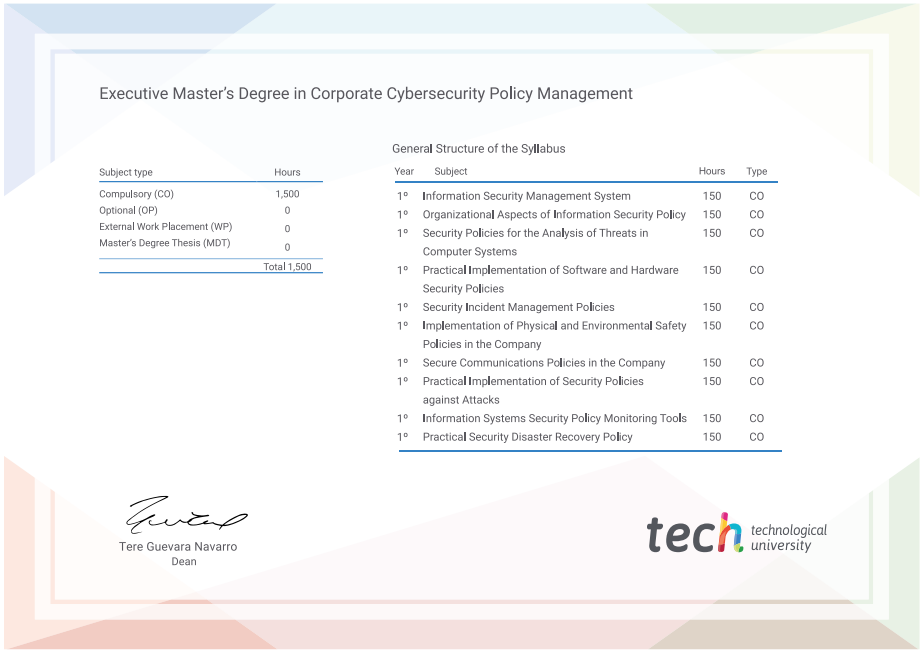
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

This qualification must always be accompanied by the university degree issued by the competent authority to practice professionally in each country. Unique TECH Code: AFWORD23S techtitute.com/certificates


Executive Master's Degree in Corporate Cybersecurity Policy Management

| Subject type | Hours |
|---|---|
| Compulsory (CO) | 1,500 |
| Optional (OP) | 0 |
| External Work Placement (WP) | 0 |
| Master's Degree Thesis (MDT) | 0 |
| | Total 1,500 |

General Structure of the Syllabus

| Year | Subject | Hours | Type |
|---|---|---|---|
| 1º | Information Security Management System | 150 | CO |
| 1º | Organizational Aspects of Information Security Policy | 150 | CO |
| 1º | Security Policies for the Analysis of Threats in Computer Systems | 150 | CO |
| 1º | Practical Implementation of Software and Hardware Security Policies | 150 | CO |
| 1º | Security Incident Management Policies | 150 | CO |
| 1º | Implementation of Physical and Environmental Safety Policies in the Company | 150 | CO |
| 1º | Secure Communications Policies in the Company | 150 | CO |
| 1º | Practical Implementation of Security Policies against Attacks | 150 | CO |
| 1º | Information Systems Security Policy Monitoring Tools | 150 | CO |
| 1º | Practical Security Disaster Recovery Policy | 150 | CO |

Tere Guevara Navarro
Dean

tech technological university

*Apostille Convention. In the event that the student wishes to have their paper certificate issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

tech technological university

# Executive Master's Degree
## Corporate Cybersecurity Policy Management

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

# Executive Master's Degree

## Corporate Cybersecurity Policy Management

MCCPM

tech technological university